Step 4: How to Configure the Load Balancer Administrative Settings

https://campus.barracuda.com/doc/3538948/

Before configuring administrative settings, complete Step 3: How to Configure the Web Interface.

Control Access to the Administration Interface

The **BASIC > Administration** page is where you perform the following tasks related to web interface access for the Barracuda Load Balancer:

- Change the password of the administration account **admin**.
- Change the port used to access the Barracuda Load Balancer web interface.
- Change the length of time after which idle users are to be logged out of the web interface (the default value is 20 minutes).
- Specify the IP addresses or netmask of the systems that can access the web administration interface. Attempts to log in as **admin** from other systems are denied.

Use the **BASIC > IP Configuration** page to allow or deny access to the web interface from the WAN and LAN IP addresses, and, optionally, to configure a management IP address.

Set the System Time Zone

You can set the time zone of your Barracuda Load Balancer from the **BASIC > Administration** page. The current time on the system is automatically updated via Network Time Protocol (NTP). When the Barracuda Load Balancer resides behind a firewall, NTP requires port 123 to be opened for outbound UDP traffic.

It is important that the time zone is set correctly because this information is used to coordinate traffic distribution and in all logs and reports.

The Barracuda Load Balancer automatically reboots when you change the time zone.

Customize the Web Interface Appearance

The **ADVANCED > Appearance** page allows you to customize the default images used on the web interface. This tab is available only on the Barracuda Load Balancer 440 and above.

Enable SSL for Administrators and Users

The **ADVANCED > Secure Administration** page allows you to configure SSL for the web interface for your Barracuda Load Balancer.

SSL not only ensures that your passwords are encrypted, but also ensures that all data transmitted to, and received from, the web interface is encrypted. You can require HTTPS to be used for secure access, and specify the certificate to be used.

> The SSL configuration referred to here is related only to the web interface. To enable SSL offloading for a Service, refer to *SSL Offloading*.

In order to only allow secured connections when accessing the web interface, you need to supply a digital SSL certificate which will be stored on the Barracuda Load Balancer. This certificate is used as part of the connection process between client and server (in this case, a browser and the web interface on the Barracuda Load Balancer). The certificate contains the server name, the trusted certificate authority, and the server's public encryption key.

The SSL certificate which you supply may be either private or trusted. A private, or self-signed, certificate provides strong encryption without the cost of purchasing a certificate from a trusted certificate authority (CA). However, the client web browser will be unable to verify the authenticity of the certificate and a warning will be sent about the unverified certificate. To avoid this warning, download the Private Root Certificate and import it into each browser that accesses the Barracuda Load Balancer web interface. You may create your own private certificate using the **ADVANCED > Secure Administration** page.

You may also use the default pre-loaded Barracuda Networks certificate. The client web browser will display a warning because the hostname of this certificate is "barracuda.barracudanetworks.com" and it is not a trusted certificate. Access to the web interface using the default certificate may be less secure. However, this certificate can be used for SMTP over TLS, so any mail messages sent by the Barracuda Load Balancer will be secure.

A trusted certificate is a certificate signed by a trusted certificate authority (CA). The benefit of this

certificate type is that the signed certificate is recognized by the browser as trusted, thus preventing the need for manual download of the Private Root Certificate.

Continue with Step 5: How to Configure the Barracuda Load Balancer Network.